## REMARKS

The claims remaining in the present application are Claims 1-20. Claims 1-9 are allowed. Claims 10-20 are rejected. The Examiner is thanked for performing a thorough search.

The Examiner is thanked for allowing Claims 1-9.

## CLAIM REJECTIONS

### 35 U.S.C. §103

Claims 10-20

Claims 10-20 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,952,779 by Cohen et al. (referred to hereinafter as "Cohen") in view of U.S. Patent Application Publication No. 2005/0022018 by Szor (referred to hereinafter as "Szor"). Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Cohen and Szor, alone or in combination.

Independent Claim 10 recites,

> A security intrusion mitigation system comprising:
> a means for communicating information;
> a means for processing information including instructions for determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path; and
> a means for storing said information, including instructions for storing information describing said highest risk path.

Independent Claim 15 recites,

> A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security intrusion mitigation instructions comprising:
> a component risk determination module for determining that a first risk of a first attack spreading from a first component to a second component is higher than a second risk of a second attack spreading from a third

component to a fourth component, wherein said first, second, third and fourth components are included in a network; and

an attack spreading response module for responding to said first risk before responding to said second risk.

Applicants respectfully assert that the combination of Cohen in view of Szor does not satisfy the requirements of a *prima facie* case of obviousness. First, Applicants respectfully submit that "[i]t is improper to combine references where the references teach away from their combination" (emphasis added; MPEP 2145(X)(D)(2); *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983)). Applicants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)). Further, Applicants respectfully submit that, "[w]ith regard to rejections under 35 U.S.C. 103, the examiner must provide evidence which as a whole shows that the legal determination sought to be proved (i.e., the reference teachings establish a *prima facie* case of obviousness) is more probable than not" (emphasis added) (MPEP 2142). In particular, "if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious" (emphasis added) (MPEP 2143.01(VI); *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)).

More specifically, Applicants respectfully submit that there is no motivation to combine the teachings of Cohen and Szor, because Cohen and Szor teach away from the suggested modification. For example, Applicants understand Cohen and Szor to change each other's principles of operation as will be described in more detail.

COHEN

Referring to the abstract and Col. 2 lines 54-60 of Cohen, among other places, Applicants understand Cohen to teach the use of a simulator as a part of

analyzing and detecting potential risks. For example, discovery agents can gather information about a network and the network's vulnerability. A simulator can receive and analyze the gathered information to determine, among other things, possible attack routes, detect flawed configurations and so on.

SZOR

Referring to the abstract and paragraph 0130 of Szor, among other places, Applicants understand Szor to teach automatically detecting malicious code on a host computer system. For example, the host computer system automatically generates and sends at least a portion of the detected malicious code to a local analysis center computer system. The local analysis center computer system provides signature updates to a network intrusion detection system based on the malicious code that the local analysis center computer system received. The local analysis center computer system automatically sends detected malicious code or malicious code signatures to a global analysis center. The global analysis center, for example, may automatically deliver signature updates to global clients.

THE COMBINATION OF COHEN AND SZOR

Applicants respectfully submit that the teachings of Szor cannot be used to modify the teachings of Cohen because Szor's teachings would change Cohen's mode of operation and vice versa. For example, Applicants understand Cohen's mode of operation to involve gathering information from a network and sending it to a simulator while Szor's mode of operation involves automatically detecting malicious code, analyzing the malicious code, and providing signature updates as a part of the on going functioning of the devices associated with Szor's network.

SUMMARY

For at least the reason that Applicants understand Cohen and Szor to teach away from each other, Applicants submit that independent Claims 10 and 15 are patentable. Claims 11-14 depend on Claim 10. Claims 16-20 depend on Claim 15. Further, these dependent claims recite additional limitations which further make

them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

## CONCLUSION

In light of the above remarks, reconsideration of the rejected claims is requested. Based on the arguments and amendments presented above, it is respectfully submitted that Claims 10-20 overcome the rejections of record. For reasons discussed herein, Applicants respectfully request that Claims 10-20 be considered be the Examiner. Therefore, allowance of Claims 10-20 is respectfully solicited.

Should the Examiner have a question regarding the instant response, the Applicants invite the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,

WAGNER BLECHER LLP

Dated: 3/27/2008

/John P. Wagner, Jr./
John P. Wagner Jr.
Registration No. 35,398


Address: Westridge Business Park
123 Westridge Drive
Watsonville, California 95076 USA

Telephone: (408) 377-0500 Voice
(408) 234-3649 Direct/Cell
(831) 722-2350 Facsimile